

Free Steiner triple systems and their automorphism groups

A. Grishkov, D. Rasskazova, M. Rasskazova, I. Stuhl

Abstract

The paper is devoted to the study of free objects in the variety of Steiner loops and of the combinatorial structures behind them, focusing on their automorphism groups.

We prove that all automorphisms are tame and the automorphism group is not finitely generated if the loop is more than 3-generated. For the free Steiner loop with 3 generators we describe the generator elements of the automorphism group and some relations between them.

1 Introduction

Steiner triple systems as special block designs are a major part of combinatorics, and there are many interesting connections developed between these combinatorial structures and their algebraic aspects. In this paper we consider Steiner triple systems from algebraic point of view, i.e., we study the corresponding Steiner loops. Diassociative loops of exponent 2 are commutative, and the variety of all diassociative loops of exponent 2 is precisely the variety of all Steiner loops, which are in a one-to-one correspondence with Steiner triple systems (see [4], p. 310).

Since Steiner loops form a variety (moreover a Schreier variety), we can deal with free objects. Consequently, we use the term *free Steiner triple systems* for the combinatorial objects corresponding to free Steiner loops. A summary of results about varieties of Steiner loops, Steiner quasigroups and free objects in the varieties can be found in [3].

We give a construction of free Steiner loops, determine their multiplication groups (which is a useful knowledge for loops, see [8], Section 1.2)). This problem for finite Steiner loops was partly solved in [12] and in [11] in the case of finite oriented Steiner loops. We also show that the nuclei of the free Steiner loops are trivial, which is an indicator of how distant these loops are from groups.

The automorphism group of a Steiner triple system \mathfrak{S} coincides with the automorphism group of the Steiner quasigroup as well as with the automorphism group of the Steiner loop associated with \mathfrak{S} . Any finite group is the automorphism group of a Steiner triple system ([7], Theorem 8, p. 103). This motivated the goal of our paper to study automorphisms of the free Steiner triple systems. We prove that (i) all automorphisms of the free Steiner loops are tame, and (ii)

2010 *Mathematics Subject Classification*: 20N05, 05B07.

Key words and phrases: Steiner triple systems, free diassociative loops, free Steiner loops, multiplication groups, automorphism groups, tame automorphisms.

the automorphism group of a free Steiner loop is not finitely generated when the loop is generated by more than 3 elements.

We also determine the generators of the automorphism group of the 3-generated free Steiner loop and give conjectures about automorphisms of this loop. These conjectures fit the context of the work [13] on linear Nielsen-Schreier varieties of algebras.

2 Preliminaries

A set L with a binary operation $L \times L \longrightarrow L : (x, y) \mapsto x \cdot y$ is called a *loop*, if for given a, b , the equations $a \cdot y = b$ and $x \cdot a = b$ are uniquely solvable, and there is an element $e \in L$ such that $e \cdot x = x \cdot e = x$ for all $x \in L$. A loop is called *diassociative* if every two elements generate a group.

A loop L is called *Steiner loop* if $x \cdot (x \cdot y) = y$ holds for all $x, y \in L$ and $x^2 = e$ for all $x \in L$, where e is the identity of L .

A *Steiner triple system* \mathfrak{S} is an incidence structure consisting of points and blocks such that every two distinct points are contained in precisely one block, and any block has precisely three points. It is a well-known fact that a Steiner triple system of order m exists if and only if $m \equiv 1, 3 \pmod{6}$ (cf. [9], Definition V.1.9).

To a given Steiner triple system, there correspond two different constructions leading distinct algebraic structures.

A Steiner triple system \mathfrak{S} determines a multiplication on the pairs of different points x, y taking as a product the third point of the block joining x and y . Defining $x \cdot x = x$ we get a *Steiner quasigroup* associated with \mathfrak{S} . Adjoining an element e with $ex = xe = x$, $xx = e$ we obtain the Steiner loop S .

Conversely, a Steiner loop S determines a Steiner triple system whose points are the elements of $S \setminus \{e\}$, and the blocks are the triples $\{x, y, xy\}$ for $x \neq y \in S \setminus \{e\}$. The quasigroup or loop obtained in this way is called an *exterior Steiner quasigroup* or an *exterior Steiner loop*. This yields the first of the aforementioned constructions. Because it is more popular than the other one, the term 'exterior' will be omitted.

To describe the second construction, let $a \in \mathfrak{S}$ be some fixed element and $IS = (\mathfrak{S}, a, \cdot)$ be a main isotope of the quasigroup associated to \mathfrak{S} via the multiplication $x \cdot y = y \cdot x = (ax)(ay)$. Then $x^2 = x \cdot x = (ax)(ax) = ax$, and hence $x^2 \cdot y^2 = xy$, $x^3 = x(ax) = a$ and $(xy)y = (x^2 \cdot y^2)^2 \cdot y^2 = x$.

Conversely, from a commutative loop S with identities $x^3 = 1$, $(x^2 y^2)^2 y^2 = x$, a Steiner triple system can be recovered, with blocks $\{x, y, x^2 y^2\}$ and $\{a, x, x^2\}$ for any $x \neq y \neq a$. This construction in a different framework appears in [3] p 23. A loop obtained in this way is called an *interior Steiner loop*.

The *left*, *right*, respectively, *middle nucleus* of a loop L are the subgroups of L defined by

$$N_l(L) = \{u; (u \cdot x) \cdot y = u \cdot (x \cdot y), x, y \in L\},$$

$$N_r(L) = \{u; (x \cdot y) \cdot u = x \cdot (y \cdot u), x, y \in L\},$$

$$N_m(L) = \{u; (x \cdot u) \cdot y = x \cdot (u \cdot y), x, y \in L\}.$$

The intersection $N(L) = N_l(L) \cap N_r(L) \cap N_m(L)$ is the *nucleus* of L .

The *commutant* $C(L)$ of a loop L is the subset consisting of all elements $c \in L$ such that $c \cdot x = x \cdot c$ for all $x \in L$. The *center* $Z(L)$ of L is the intersection $C(L) \cap N(L)$.

For any $x \in L$ the maps $\lambda_x : y \mapsto x \cdot y$ and $\rho_x : y \mapsto y \cdot x$ are the *left* and the *right translations*, respectively. The permutation group generated by the left and right translations of loop L is called the *multiplication group* of L , and the stabilizer of the neutral element is called the *inner mapping group* of L . These basic facts can be found in [2].

3 Free Steiner loops

Constructions of free Steiner loops have been given by several authors: see e.g., [3], [6]. Nevertheless, we provide here a specific construction; it will help to incorporate a transparent interpretation and to establish a natural system of notation.

Let \mathbf{X} be a finite ordered set and let $W(\mathbf{X})$ be a set of non-associative \mathbf{X} -words. The set $W(\mathbf{X})$ has an order such that $v > w$ if and only if $|v| > |w|$ or $|v| = |w| > 1$, $v = v_1 v_2$, $w = w_1 w_2$, $v_1 > w_1$ or $v_1 = w_1, v_2 > w_2$. Next, we define the set $S(\mathbf{X})^* \subset W(\mathbf{X})$ of S -words by induction on the length of word:

- $\mathbf{X} \subset S(\mathbf{X})^*$,
- $vw \in S(\mathbf{X})^*$ precisely if, $v, w \in S(\mathbf{X})^*$, $|v| \leq |w|$, $v \neq w$ and if $w = w_1 \cdot w_2$, then $v \neq w_i$, ($i = 1, 2$).

On $S(\mathbf{X}) = S(\mathbf{X})^* \cup \{\emptyset\}$ we define a multiplication in the following manner:

1. $v \cdot w = w \cdot v = vw$ if $vw \in S(\mathbf{X})$,
2. $(vw) \cdot w = w \cdot (vw) = w \cdot (wv) = (wv) \cdot w = v$,
3. $v \cdot v = \emptyset$.

A word $v(x_1, x_2, \dots, x_n)$ is *irreducible*, if $v \in S(\mathbf{X})^*$.

Proposition 1 *The set $S(\mathbf{X})$ with the multiplication as above is a free Steiner loop with free generators \mathbf{X} .*

Proof. The definition implies that $S(\mathbf{X})$ is commutative, $a \cdot (a \cdot b) = b$ for all $a, b \in S(\mathbf{X})$ and if $a, b \in S(\mathbf{X})$ then $\{a, b, a \cdot b, \emptyset\}$ is a group of order 4 and exponent 2. Hence $S(\mathbf{X})$ is free diassociative of exponent 2, i.e., a free Steiner loop. ■

Let (G, H, B) be a Baer triple (see [1]), i.e., $G = BH$ is a group, H is a subgroup in G , B is a set of representatives for G/H with $b^2 = 1, b \in B, B \cap H = 1$, and for any $b_1, b_2 \in B$ there exists $b_3 \in B$ such that $b_1 b_2 = b_3 h_1$, $b_2 b_1 = b_3 h_2$, where $h_1, h_2 \in H$.

Define a multiplication on B by $b_1 * b_2 = b_3 = b_2 * b_1$. Clearly $b * b = 1$ and $(b_1 * b_2) * b_2 = b_1$. Indeed, $(b_1 * b_2) * b_2 = b_3 * b_2 = b_2 * b_3 = b_2 * (b_2 b_1 h_2^{-1}) = b_1$ since $b_2 b_2 b_1 h_2^{-1} = b_1 h_2^{-1}$. This yields that $(B, *)$ is a Steiner loop. We call such a decomposition $G = BH$ an *S-decomposition*.

If the intersection $\bigcap_{x \in G} H^x = \{1\}$ then $G \simeq \text{Mult}((B, *))$.

We note that any Steiner loop can be constructed in the above fashion. Indeed, let $G = \text{Mult}(B)$ be the multiplication group of the Steiner loop B and let $B_0 = \{R_b | b \in B\}$, $H = \langle R_a R_b R_{ab} | a, b \in B \rangle$. Then $G = B_0 H$ is an S-decomposition.

Proposition 2 *Let $G = \text{Mult}(S(\mathbf{X}))$ be the group of right multiplications of the free Steiner loop $S(\mathbf{X})$. Then*

1. $G = \bigast_{v \in S(\mathbf{X})} C_v$ is a free product of cyclic groups of order 2;
2. G acts on $S(\mathbf{X})$, and $G = \{R_v | v \in S(\mathbf{X})\} \text{Stab}_G(\emptyset)$. Moreover, the inner mapping group $\text{Stab}_G(\emptyset)$ is a free subgroup of G generated by $R_v R_w R_{vw}$, $v, w \in S(\mathbf{X})$.

Proof. The claims follow from the consideration above and from the definition of the free product of groups or this fact can be found in [10] Sec. 11.3.

The subgroup $\text{Stab}_G(\emptyset)$ is free by the Kurosh subgroup theorem [5] p. 17. ■

Proposition 3 *If x, y are different elements of the free Steiner loop $S(\mathbf{X})$ and $|\mathbf{X}| > 2$, then there is an element $z \in S(\mathbf{X})$ such that*

$$(xy)z \neq x(yz).$$

Proof. Let $x = v_1(x_1, \dots, x_n)$ and $y = v_2(x_1, \dots, x_n)$. Suppose we choose the element z in the shape $z = v_2(x_1, \dots, x_n) \cdot x_j$, where x_j is one of the generators different from the last letter of $v_2(x_1, \dots, x_n)$. Then we have that

$$(xy)z = (v_1(x_1, \dots, x_n) \cdot v_2(x_1, \dots, x_n))(v_2(x_1, \dots, x_n)x_j)$$

$$\neq v_1(x_1, \dots, x_n) \cdot (v_2(x_1, \dots, x_n) \cdot v_2(x_1, \dots, x_n)x_j) = v_1(x_1, \dots, x_n)x_j = x(yz).$$

■

As was mentioned earlier, the nucleus of a loop can be interpreted as a 'measure' of the non-associativity. As a corollary of the previous Proposition, we can conclude that the free Steiner loops are 'very far' from groups:

Corollary 4 *The nucleus and therefore the center of free Steiner loops are trivial.*

4 Automorphisms

Let $\mathbf{Y} = \{y_1, y_2, \dots, y_n\}$ be a set of free generators of $S(\mathbf{X})$. Then $\varphi : \mathbf{Y} \rightarrow S(\mathbf{X})$, $\varphi(y_1) = y_1 \cdot v$, $\varphi(y_i) = y_i$, ($i = 2, \dots, n$), $v \in S(\mathbf{Y} \setminus y_1)$ is an automorphism of $S(\mathbf{X})$, called an *elementary automorphism* (or an *Y-elementary automorphism*) and we will denote it by $\varphi = e_i(v)$. Let $T(\mathbf{X})$ denote a subgroup of the group of automorphisms $\text{Aut}(S(\mathbf{X}))$ of loop $S(\mathbf{X})$ generated by the \mathbf{X} -elementary automorphisms. Automorphisms contained in $T(\mathbf{X})$ are called *tame* (or \mathbf{X} -tame). In Theorem 7 below we show that $\text{Aut}(S(\mathbf{X})) = T(\mathbf{X})$.

Let $\mathbf{Y} = \{y_1, y_2, \dots, y_m\} \subset S(\mathbf{X})$, then set \mathbf{Y} is said to be *reducible*, if there exist i and $v \in S(\mathbf{Y} \setminus y_i)$ such that $|y_i \cdot v| < |y_i|$.

Let $S(Z)$ be a free Steiner loop with free generators $Z = \{z_1, \dots, z_m\}$, let $Y = \{y_1, \dots, y_m\}$ be a set of elements of $S(X)$ and let $\varphi : S(Z) \longrightarrow S(Y) : z_i \mapsto y_i$ be a homomorphism. A set Y is called *free isometric*, if φ is an isomorphism and $|\varphi(v(z_1, \dots, z_m))| = \|v(z_1, \dots, z_m)\|$. Here $\|v(z_1, \dots, z_m)\|$ is the length with weights $|y_1|, \dots, |y_m|$, it means that $\|z_i\| = |y_i|$.

Proposition 5 *A set Y is irreducible if and only if Y is free isometric.*

Proof. Let Y be an irreducible subset of $S(X)$, $S(Z)$ be a free Steiner loop with free generators $Z = \{z_1, \dots, z_m\}$ and let $\varphi : S(Z) \longrightarrow S(Y) : z_i \mapsto y_i$ be a homomorphism. We show that φ is an isometric isomorphism.

Let us choose $v \in \text{Ker}\varphi$ of minimal length and set $v = v_1 \cdot v_2$, then $\varphi(v_1) = \varphi(v_2)$. Assume that $v_1 = w_1 \cdot w_2$ and $v_2 = w_3 \cdot w_4$ are irreducible, then we have $\varphi(w_1) \cdot \varphi(w_2) = \varphi(w_3) \cdot \varphi(w_4)$. Suppose that these decompositions are irreducible. Then we get that $\varphi(w_4) = \varphi(w_1)$ or $\varphi(w_4) = \varphi(w_2)$. This yields a contradiction with the minimality of the choice of v in both cases.

Now we assume, that the decomposition $\varphi(w_1) \cdot \varphi(w_2)$ is reducible, then $\varphi(w_1) = u_1 \cdot \varphi(w_2)$. Hence $u_1 = \varphi(w_5)$ and $\varphi(w_1) = \varphi(w_5 \cdot w_2)$. Since the decomposition $w_1 \cdot w_2$ is irreducible, $w_1 = w_6 \cdot w_7$, $\varphi(w_6) = w_5$ and $\varphi(w_7) = \varphi(w_2)$. Moreover, $w_7 \neq w_2$ and therefore $w_2 \cdot w_7 \in \text{Ker}\varphi$ and $|w_2 \cdot w_7| > |v_1 \cdot v_2|$. But since $|v_1| > |w_2|$, we have $|v_2| < |w_7| < |w_1| < |v_1|$. This proves the assertion. ■

Corollary 6 *If Y is irreducible then $S(Y) = S(X)$ precisely if $Y = X$.*

Later on we will prove that all automorphisms of the free Steiner loops are tame.

Theorem 7 *Let $S(X)$ be a free Steiner loop with free generators X . Then $\text{Aut}(S(X)) = T(X)$.*

Proof. Let φ be an automorphism of $S(X)$ and let $Y = \varphi(X)$. We prove that $\varphi \in T(X)$ by induction on $|Y| = \sum_{i=1}^n |y_i|$.

First we note that the permutations of X are tame automorphisms. For any transposition $(ij) \in \mathcal{S}_n(X)$ we have $(ij) = \phi\psi\phi$ with

$$\phi = e_i(x_j) \quad \text{and} \quad \psi = e_j(x_i).$$

Since the symmetric group $\mathcal{S}_n(X)$ of permutations of X is generated by transpositions, one has $\mathcal{S}_n(X) \subset T(X)$.

If $|Y| = n$ then $\varphi \in \mathcal{S}_n(X)$ and therefore $\varphi \in T(X)$. Now suppose that $|Y| > n$. By Corollary 6 the set Y is reducible and hence for some i and $v = v(y_1, \dots, \widehat{y_i}, \dots, y_n)$ we have $|y_i \cdot v| < |y_i|$. By the induction assumption the map $\psi(x_1, \dots, x_n) = (y_1, \dots, y_{i-1}, y_i \cdot v, \dots, y_n)$ induces an X -tame automorphism of $S(X)$. Set

$$w = v(y_1, \dots, \widehat{y_i}, \dots, y_n)^{\psi^{-1}} = v(x_1, \dots, \widehat{x_i}, \dots, x_n).$$

Then $\lambda(x_1, \dots, x_i, \dots, x_n) = (x_1, \dots, x_i \cdot w, \dots, x_n)$ is an X -elementary automorphism. Then $\varphi = \lambda\psi$ since $x_j^{\lambda\psi} = x_j^\psi = y_j$ for $j \neq i$ and $x_i^{\lambda\psi} = (x_i \cdot w)^\psi = (y_i \cdot v) \cdot w^\psi = (y_i \cdot v) \cdot v = y_i$.

Consequently, $\varphi \in T(X)$; this completes the proof of the theorem. ■

Lemma 8 *Let $\phi = e_i(v)$, $v \in S(\mathbf{X} \setminus i)$ be an \mathbf{X} -elementary automorphism and suppose $u = u_1 u_2$ is an \mathbf{X} -irreducible decomposition of a word $u \in S(\mathbf{X})$. Then either $u_1^\phi u_2^\phi$ is an \mathbf{X} -irreducible decomposition of u^ϕ or $u^\phi = x_i$, in which case $u_1 = x_i$ and $u_2 = v$.*

Proof. We will use induction in the length $|u|$ of the word u . First suppose that $u_1^\phi u_2^\phi$ is an \mathbf{X} -reducible decomposition of u^ϕ . It means that $u_1^\phi = u_3 u_2^\phi$ is also an \mathbf{X} -irreducible decomposition, and hence $u_1 = u_3^\phi u_2$. If $u_1 = u_3^\phi u_2$ is an \mathbf{X} -irreducible decomposition then $u = u_1 u_2$ is \mathbf{X} -reducible, which yields a contradiction.

Therefore, $u_1 = u_3^\phi u_2$ is \mathbf{X} -reducible, where $u_1 = x_i$, $u_2 = v$, $u_3 = x_i$. Suppose $|u_3| > 1$, $|u_2| > 1$, $u_3 = wx_i$ and $u_2 = yv$ ($w \neq x_i \neq v \neq y$). Then $u_3^\phi u_2 = [w(x_i v)] \cdot yv$ is \mathbf{X} -reducible if and only if $w = yv$ or $x_i = y$. In the first case we get that $u_1^\phi u_2^\phi = x_i \cdot yv$ is \mathbf{X} -irreducible. In the second case $u_1 = u_3^\phi u_2 = w$ and $u_1 u_2 = w(x_i v)$ is \mathbf{X} -irreducible. Hence, $u_1^\phi u_2^\phi = wx_i$ is also \mathbf{X} -irreducible decomposition of u^ϕ . ■

Define a normal chain of characteristic ($\text{Aut}(S(\mathbf{X}))$ -invariant) subloops of $S(\mathbf{X})$:

$$S_0 = S(\mathbf{X}) > S_1 > S_2 > \cdots > S_i > \cdots \quad (1)$$

Here S_0/S_1 is a group, and for any i , $Z_i = S_i/S_{i+1}$ is the center of the factor loop S_0/S_{i+1} . Moreover, each S_i is a minimal subloop with these properties.

Now we deal with the question whether the automorphism group of a free Steiner loop with n generators is finitely generated for $n > 3$.

Theorem 9 *The automorphism group $\text{Aut}(S(\mathbf{X}))$ of the free Steiner loop $S(\mathbf{X})$ is not finitely generated when $|\mathbf{X}| > 3$.*

Proof. Owing to Theorem 7 and by a discussion afterwards, the group $G = \text{Aut}(S(\mathbf{X}))$ is generated by $\{e_i(v) | v \in S(\mathbf{X})\}$. If G is finitely generated then G is generated by a set $P = \{e_{j_i}(v_i) | v_i \in S(\mathbf{X}), i = 1, \dots, m\}$.

Let $S(\mathbf{X}) > S_1 > S_2 > \cdots > S_i > \cdots$ be a chain of normal characteristic subloops as in Eqn (1). Choose a number p such that $v_i \notin S_p$, $i = 1, \dots, m$, and $1 \neq v \in S_p$. We assume that

$$e_j(v) = e_{j_1}(v_1) \cdots e_{j_m}(v_m).$$

For any $w \in S(\mathbf{X})$ we set (i) $\|w\| = (s, t)$, if $w = w_1 w_2$ is an \mathbf{X} -irreducible decomposition, $w_1 > w_2 \neq 1$, $w_1 \in S_s \setminus S_{s+1}$, $w_2 \in S_t \setminus S_{t+1}$ and (ii) $\|x\| = (1, 0)$, if $x \in \mathbf{X}$.

We prove that $\|x_j e_{j_1}(v_1) \cdots e_{j_r}(v_r)\| = (1, s)$, with $s < m$, by induction in r . For $r = 1$ this is clear, and we suppose that for r this fact is true.

Set:

$$u = x_1 e_{j_1}(v_1) \cdots e_{j_r}(v_r) e_i(w), \quad q = x_1 e_{j_1}(v_1) \cdots e_{j_r}(v_r) = q_1 q_2.$$

By the induction hypothesis we have $\|q_1\| = 1$, $\|q_2\| = s < m$.

If $q_1^{e_i(w)} q_2^{e_i(w)}$ is an \mathbf{X} -irreducible decomposition then $\|q^{e_i(w)}\| = \|q\| = (1, s)$, since S_s is a characteristic subloop. If $q_1^{e_i(w)} q_2^{e_i(w)}$ is an \mathbf{X} -reducible

decomposition then, by Lemma 8, $q^{e_i(w)} = u = x_i$ and $\|u\| = (1, 0)$. We obtain that $x_j^{e_j(v)} = x_j v$ and $\|x_j e_{j_1}(v_1) \cdots e_{j_m}(v_m)\| = (1, s)$, with $s < m$. However, this contradicts to the fact $\|x_j v\| = (1, m)$. This completes the inductational step.

Therefore our assumption that G is finitely generated does not hold. ■

The group $\text{Aut}(S(\mathbf{X})) = T(\mathbf{X})$ is generated by \mathbf{X} -elementary automorphisms $e_i(v)$, $v \in S(\mathbf{X} \setminus \{i\})$, with $e_i(v)^2 = 1$; this follows from the definition. Thus, a natural question arises:

Problem 1. Which relations exist between \mathbf{X} -elementary automorphisms of the free Steiner loop $S(\mathbf{X})$?

We stress, that there is no relation between the elements $\{e_i(v) | v \in S(\mathbf{X} \setminus x_i)\}$.

In what follows we focus on the 3-generated free Steiner loop $S(x_1, x_2, x_3)$. Contrary to the case of the automorphism group of free Steiner loop with $n > 3$ -generators, we prove that the group $\text{Aut}(S(x_1, x_2, x_3))$ is generated by three involutions (12), (13) and $\varphi = e_1(x_2)$.

Theorem 10 *Let $S(\mathbf{X})$ be a free Steiner loop with free generators $\mathbf{X} = \{x_1, x_2, x_3\}$. Then the group of automorphisms $\text{Aut}(S(\mathbf{X}))$ is generated by the symmetric group \mathcal{S}_3 and by the elementary automorphism $\varphi = e_1(x_2)$.*

Proof. Let G_0 be the subgroup of $\text{Aut}(S(\mathbf{X}))$ generated by \mathcal{S}_3 and φ . If G_0 is a proper subgroup, then let ϕ be an element of $\text{Aut}(S(\mathbf{X})) \setminus G_0$. The length of $\phi(x_1, x_2, x_3) = (u, v, w)$ is the sum of the length of the generators under ϕ , i.e., $|\phi| = |u| + |v| + |w|$.

The claim of Theorem 10 can be verified by induction on the length of element $\phi \in \text{Aut}(S(\mathbf{X})) \setminus G_0$. For $|\phi| = 3$, it is trivial. Now if $|\phi| > 3$ then by the induction hypothesis we have that if $|\psi| < |\phi|$ then $\psi \in G_0$. By Corollary 6 the collection $\{u, v, w\}$ is reducible, and we can suppose that $u = u_0 \cdot u_1$, $u_1 \in \{v, w, v \cdot w\}$. There is an automorphism α such that $\alpha(x_1, x_2, x_3) = (u_0, v, w)$; $\alpha \in G_0$ since $|\alpha| < |\phi|$. If $u = u_0 \cdot v$ then $\phi = \varphi\alpha$. Further, if $u = u_0 \cdot (v \cdot w)$ then

$$\phi = (13)\varphi(123)\varphi(132)\varphi(13)\alpha. \quad (2)$$

Finally, if $u = u_0 \cdot w$ then $\phi = (23)\varphi(23)\alpha$. In all three cases ϕ is contained in the group G_0 ; this implies the assertion of the theorem. ■

Theorem 10 implies

Corollary 11 *Let $S(\mathbf{X})$ be the Steiner loop with free generators $\mathbf{X} = \{a, b, c\}$. Let Q be the stabilizer $\text{Stab}_{\text{Aut}(S(\mathbf{X}))}(c)$ of element c in the automorphism group of $S(\mathbf{X})$. Then*

$$Q = \langle \varphi, \tau, \xi \rangle$$

with

$$\varphi(a, b, c) = (ab, b, c), \quad \xi(a, b, c) = (ac, b, c), \quad \tau(a, b, c) = (b, a, c).$$

Proof. Denote by Q_0 the subgroup of Q generated by ξ, φ, τ and let $\lambda \in Q$ be the map $\lambda(a, b, c) = (v, w, c)$, with $|\lambda| = |v| + |w|$. Suppose that for every $\gamma \in Q$ with $|\gamma| < |\lambda|$, γ is contained in Q_0 .

Since (v, w, c) is reducible, we have three possibilities: $v = v_0w$, $v = v_0c$ or $v = v_0(wc)$.

Consider the map $\lambda_0(a, b, c) = (v_0, w, c)$; it is contained in Q_0 by induction because $|\lambda_0| < |\lambda|$.

In the first case $\lambda = \varphi\lambda_0$. In the second case $\lambda = \xi\lambda_0$, and for the mapping $\phi(a, b, c) = (a(bc), b, c)$ we have by Eqn (2) (see the proof of Theorem 10). In the third case $\phi = \tau\xi\varphi\tau\varphi\xi\tau \in Q_0$.

In each case $\lambda \in Q_0$; this fact yields that $Q_0 = Q$. ■

Let us return to Problem 1. As was mentioned in the proof of Theorem 10, any transposition of the symmetric group $\mathcal{S}_n(\mathbf{X})$ on \mathbf{X} can be written as a product of \mathbf{X} -elementary automorphisms

$$(ij) = e_i(x_j)e_j(x_i)e_i(x_j).$$

Using this description of translations and the equation

$$(i-1, i)(i, i+1)(i-1, i) = (i, i+1)(i-1, i)(i, i+1),$$

we get that

$$\begin{aligned} e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i)e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1})e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i) = \\ e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1})e_{i-1}(x_i)e_i(x_{i-1})e_{i-1}(x_i)e_i(x_{i+1})e_{i+1}(x_i)e_i(x_{i+1}). \end{aligned}$$

This yields the relation

$$(e_i(x_j)e_j(x_i))^3 = 1.$$

In the proof of Theorem 10 we showed a further relation

$$\begin{aligned} e_1(x_2 \cdot x_3) &= (13)\varphi(123)\varphi(132)\varphi(13) = \\ e_1(x_3)e_3(x_1)e_1(x_3)e_2(x_1)e_1(x_2)e_1(x_3)e_3(x_1)e_1(x_3)e_1(x_2)e_1(x_3)e_3(x_1) \\ &\cdot e_1(x_3)e_1(x_2)e_2(x_1)e_1(x_3)e_3(x_1)e_1(x_3)). \end{aligned}$$

These facts suggest the following

Conjecture 12 *The group $\text{Aut}(S(x_1, x_2, x_3))$ is generated by three involutions $(12), (13)$ and $\varphi = e_1(x_2)$ with relations*

$$(12)(13)(12) = (13)(12)(13), \quad (\varphi(12))^3 = (\varphi(13))^4 = 1.$$

The analysis of computerised calculations shows that if the Conjecture 12 is false then some new relations might exist, between the above involutions, of the type

$$\varphi\sigma_1\varphi\sigma_2 \cdots \varphi\sigma_n = 1.$$

Here $\sigma_i \in S_3 = \langle (12), (13) \rangle$. Moreover, $\sigma_i \neq (12)$ or 1 ; if $\sigma_i = (13)$ then $\sigma_{i+1} \neq (13)$. Finally, $n > 50$ (for $n \leq 50$ new relations were not found).

In paper [13] it has been proved that the automorphism group of a free algebra of an arbitrary linear Nielsen–Schreier variety is generated by elementary automorphisms with some specific relations (2)–(4) ([13], pages 210–211). If Conjecture 12 holds, we will have a similar result for the group $\text{Aut}(S(\mathbf{X}))$ of the free Steiner loop $S(\mathbf{X})$ in the case $|\mathbf{X}| = 3$.

Remark 13 If Conjecture 12 is true, group $\text{Aut}(S(x_1, x_2, x_3))$ is the Coxeter group $\langle (12), (13), \varphi \mid (\varphi(12))^3 = (\varphi(13))^4 = ((12)(13))^3 = 1 \rangle$.

Conjecture 14 $Q = \{\varphi, \tau, \xi \mid \xi^2 = \varphi^2 = \tau^2 = (\tau\varphi)^3 = 1\}$.

Theorem 15 If Conjecture 12 is true then Conjecture 14 is also true.

Proof. Suppose that Conjecture 12 is true but Conjecture 14 is not. Then there exists a non-trivial word $w = w_1 \dots w_n$ formed by the letters $\{\tau, \xi, \varphi\}$ such that $a^w = a, b^w = b$. Here the "non-trivial" means that w does not contain the subwords $\varphi\tau\varphi$ and $\xi\tau\xi\tau$.

Applying induction in n , assume that for any non-trivial word v constructed from $\{\tau, \xi, \varphi\}$, of length less than n , the corresponding word in $\{\tau, \pi, \varphi\}$ is non-trivial, where $\pi = (23)$. Observe that $\xi = \pi\varphi\pi$. Hence, $w_0 = w_1 \dots w_{n-1}$ is a non-trivial word in $\{\tau, \pi, \varphi\}$. We focus on the case where no non-trivial word. The choice $w_{n-1} = \tau$ implies that $w_n \neq \tau$ and $w_{n-2} \neq \tau$. Furthermore, if $w_n = \xi = \pi\varphi\pi$ then $w = w_1 \dots w_{n-2}\tau\pi\varphi\pi$ is a non-trivial word in $\{\tau, \pi, \varphi\}$. If $w_n = \varphi$ and $w_{n-2} = \xi$ then w is again a non-trivial word in $\{\tau, \pi, \varphi\}$. Finally, if $w_n = \varphi$ and $w_{n-2} = \varphi$ then w is not a non-trivial word in $\{\tau, \xi, \varphi\}$, since w contains the subword $w_{n-2}w_{n-1}w_n = \varphi\tau\varphi$. ■

Next, we present as a consequence of the preliminary results, a connection between the groups of automorphisms of (a) free Steiner quasigroups and their associated (b) the free exterior Steiner loops and free interior Steiner loops.

Theorem 16 Let $S(\mathbf{X})$ be a free Steiner quasigroup with free generators \mathbf{X} . Let $ES(\mathbf{X}) = S(\mathbf{X}) \cup e$ and $IS(\mathbf{X})$ be its corresponding free exterior and interior Steiner loop, respectively.

Then $\text{Aut}(S(\mathbf{X})) = \text{Aut}(ES(\mathbf{X}))$ and $\text{Aut}(IS(\mathbf{X})) \simeq \text{Stab}_{\text{Aut}(ES(\mathbf{X}))}(a)$, where $a \in IS(\mathbf{X})$ is the unit element of loop $IS(\mathbf{X})$.

Acknowledgement

Izabella Stuhl has been supported by FAPESP Grant - process number 11/51845-5, and expresses her gratitude to IMS, University of São Paulo, Brazil, for the warm hospitality.

References

- [1] R. Baer, Nets and Groups, *Trans. Am. Math. Soc.*, 46, (1939), 110-141.
- [2] O. Chein, Examples and methods of construction, in *Quasigroups and Loops: Theory and Applications*, ed. O. Chein, H.O. Pflugfelder, J.D.H. Smith, Heldermann Verlag, Berlin, (1990), 27-95.
- [3] T. Evans, Varieties of loops and quasigroups, in *Quasigroups and Loops: Theory and Applications*, ed. O. Chein, H.O. Pflugfelder, J.D.H. Smith, Heldermann Verlag, Berlin, (1990), 1-26.
- [4] B. Ganter, U. Pfüller, A remark on commutative di-associative loops, *Algebra Universalis*, 21, (1985), 310-311.

- [5] A.G. Kurosh, The theory of groups, Vol. 2., *Chelsea publishing company, New York (1960)*.
- [6] S. Markovski, A. Sokolova, Free Steiner loops, *Glasnik Matematički*, 36, (2001) 85-93.
- [7] E. Mendelsohn, On the Groups of Automorphisms of Steiner Triple and Quadruple Systems, *J. of Combinatorial Theory*, 25 Ser.A, (1978) 97-104.
- [8] P. T. Nagy, K. Strambach, Loops in Group Theory and Lie Theory, *Expositions in Mathematics* 35, *Walter de Gruyter, Berlin-New York (2002)*.
- [9] H. O. Pflugfelder, Quasigroups and Loops: Introduction, *Heldermann Verlag, Berlin (1990)*.
- [10] J. D. Smith, An introduction to Quasigroups and Their Representations, *Chapman Hall/CRC, Boca Raton, FL, (2006)*.
- [11] K. Strambach, I. Stuhl, Oriented Steiner loops, *Beiträge zur Algebra und Geometrie*, 54, (2013) 131-145.
- [12] K. Strambach, I. Stuhl, Translation groups of Steiner loops, *Discrete Mathematics*, 309, (2009) 4225-4227.
- [13] U. U. Umirbaev, Defining relations for automorphism groups of free algebras, *Journal of Algebra*, 314, (2007) 209-225.

Alexander Grishkov
 Institute of Mathematics and Statistics
 University of São Paulo
 05508-090 São Paulo, SP, Brazil
E-mail: grishkov@ime.usp.br

Diana Rasskazova
 Novosibirsk State University
 630090 Novosibirsk, Russia
E-mail: ivakirjan@gmail.com

Marina Rasskazova
 Omsk Service Institute
 644099 Omsk, Russia
E-mail: marinarasskazova1@gmail.com

Izabella Stuhl
 Institute of Mathematics and Statistics
 University of São Paulo
 05508-090 São Paulo, SP, Brazil
 University of Debrecen
 H-4010 Debrecen, Hungary
E-mail: izabella@ime.usp.br